



Environnements de TP pour la sécurité

Bruno Martin

RESSI'19, le 16 mai

UNIVERSITÉ
CÔTE D'AZUR

Présentation générale

Environnement physique

Techniques de virtualisation

Hyperviseur de type 2

Hyperviseur de type 1 virtualisé

Hyperviseur de type 1 (serveur)

Conclusion

UNIVERSITÉ
CÔTE D'AZUR



Présentation générale

UNIVERSITÉ
CÔTE D'AZUR

Permettre aux étudiants d'utiliser :

- une distribution d'audit (Kali, BlackArch, Parrot) en étant root sur la distribution et sur le(s) réseau(x)
- un serveur (passerelle sous Ubuntu) pour ajouter des services
- un client sous BSD

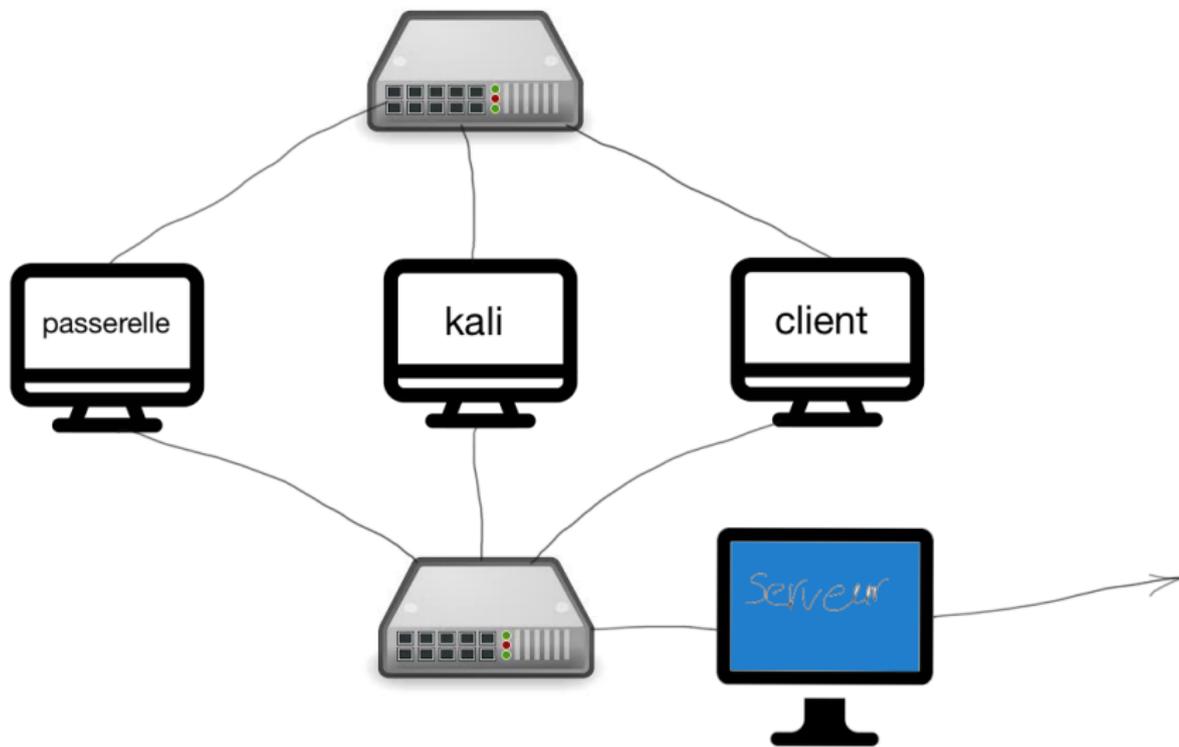
Toutes ces machines reliées sur 1 (ou 2) LAN et **en toute sécurité**.

Exemples de TP à réaliser

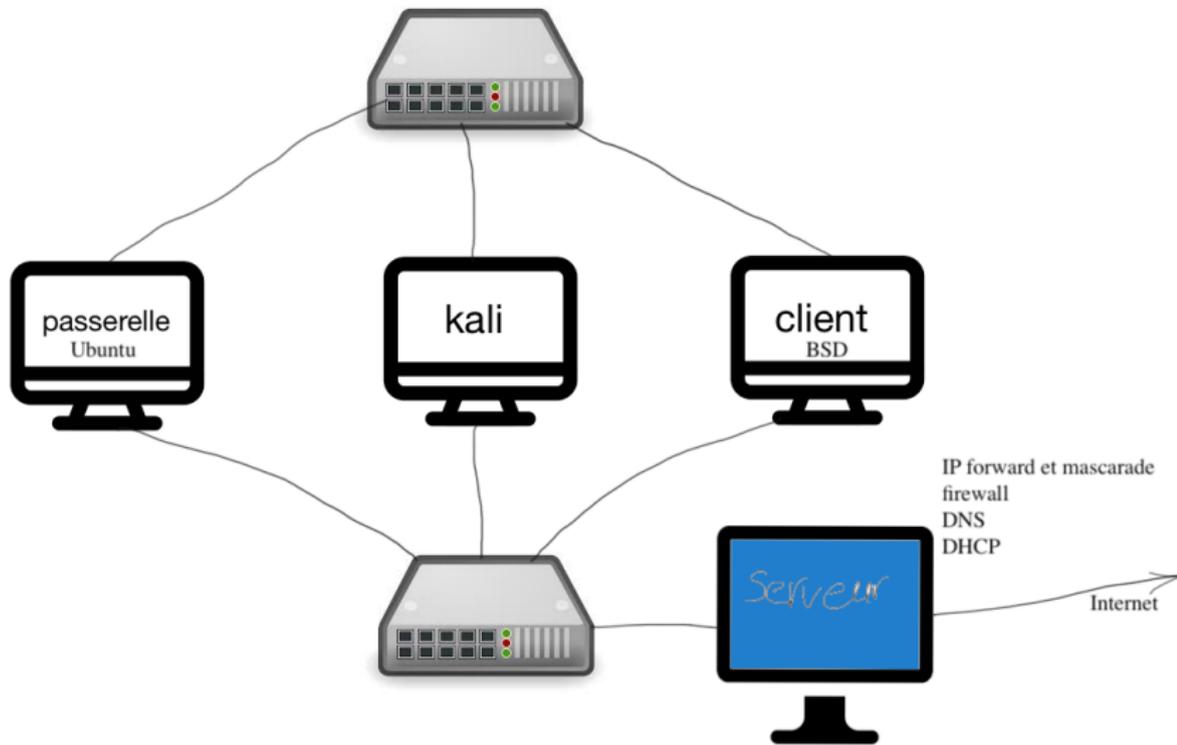
- Utiliser le serveur relié à 2 interfaces réseau comme passerelle (IP forwarding, IP masquerading)
- Installer un serveur web (http et https), publier un formulaire de login et réaliser une attaque MIM (démon)
- Installer un serveur smtp, imap(s), configurer le smtp client, réaliser des attaques MTA et sur le serveur imap(s) ; utiliser GPG
- Mettre en place openVPN en mode routé puis ponté, tenter de réaliser des attaques
- Réaliser un mini audit sur le serveur en utilisant OpenVAS, nmap et Metasploit

En mettant en place au fur et à mesure les règles de firewall et en assurant la sécurité

Environnement de TP



Environnement de TP



Au moins 4 façons de réaliser l'environnement de TP :

- physiquement : avec un serveur, des commutateurs réseaux, des machines physiques
- virtuellement sur un ordinateur personnel avec :
 - un hyperviseur de type 2
 - un hyperviseur de type 1 virtualisé
- virtuellement sur un serveur de virtualisation

UNIVERSITÉ
CÔTE D'AZUR



Environnement physique

UNIVERSITÉ
CÔTE D'AZUR

Environnement physique

Entre 2000 et 2009 dans une salle séparée du réseau par un serveur, un parc de 24 machines (12 avec 2 NIC, 12 avec 1 NIC) sur un réseau commuté reconfigurable.

- + Réinstallation rapide (technique de kickstart de Fedora)
- + Possibilité d'ajouter des équipements (routeur wifi)
- Salle dédiée non utilisable pour d'autres TP
- (Seulement) 2 machines par étudiant : passerelle et client
- Mises à jour laborieuses
- Plus de services sur le serveur (reconfiguration réseau, ...)
- Coût élevé

Pas de remplacement des machines \mapsto passage à la virtualisation.



Techniques de virtualisation

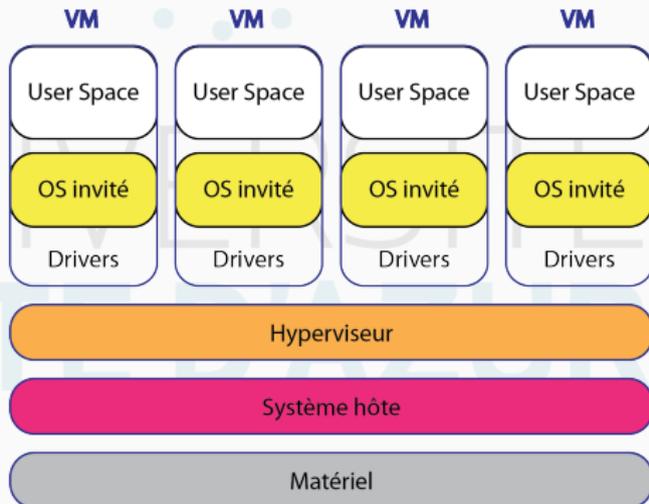
UNIVERSITÉ
CÔTE D'AZUR

Machine virtuelle – Hyperviseur de type 2

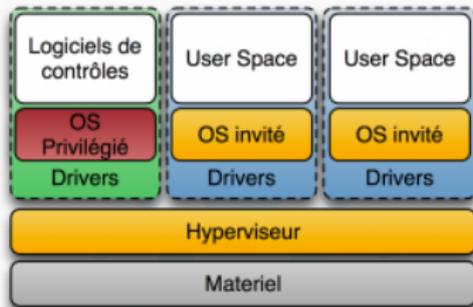
Un logiciel émule le matériel et permet de lancer plusieurs OS invités sur le système hôte physique. La mémoire et le CPU sont directement accessibles aux VM. On parle d'**hyperviseur de type 2**.

Technique qui fait cohabiter plusieurs OS isolés qui communiquent par un réseau émulé.

- KVM
- QEMU
- **VMware**
- VirtualBox
- VirtualPC
- Bochs



Hyperviseur de type 1



L'hyperviseur est un noyau système léger et optimisé pour la gestion de noyaux des SE invités directement au dessus de la couche matérielle. On parle d'**hyperviseur de type 1** ou natif ou baremetal.

- VMware ESX, ESXi
- Xen qui est utilisé en particulier dans QubesOS

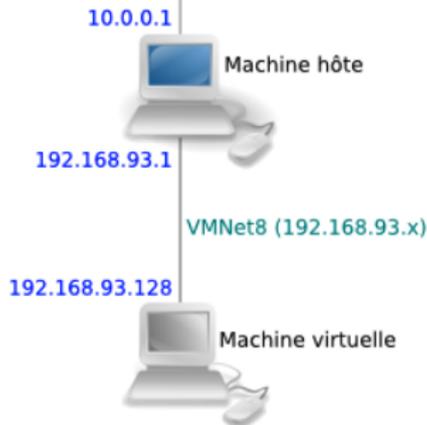
3 modes de fonctionnement principaux

- **NAT** : fonctionnement le plus simple. La VM se comporte comme un hôte connecté à un routeur qui acquiert son IP par dhcp. Le logiciel de virtualisation sert de routeur.
- **Host only** : la VM ne peut communiquer qu'avec d'autres VM hébergées sur le même hôte, comme si elles étaient connectées par un commutateur.
- **Bridge** : partage l'interface physique de la machine hôte. La VM acquiert son IP par un serveur externe à l'hôte.

	accès au LAN	adr. IP de LAN
host only	NON	NON
NAT	OUI	NON
Bridge	OUI	OUI

Mise en réseau NAT & Host only

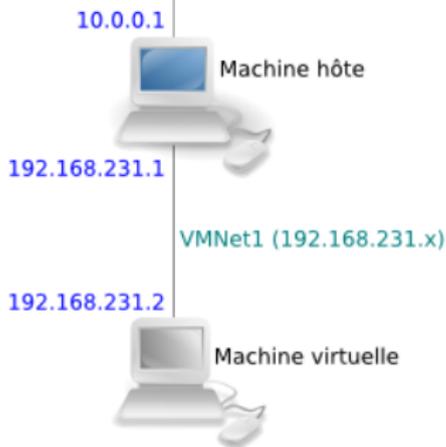
LAN (10.0.0.x)



NAT

La machine virtuelle a accès au LAN à travers la machine hôte par un routage de type NAT (Network Address Translation).
Vu du LAN, il n'y a aucune nouvelle machine.
La machine virtuelle envoie ses requêtes sur le LAN en utilisant l'adresse IP de la machine hôte.
Nécessite un LAN opérationnel et connecté.
La machine hôte fait office de serveur DHCP pour le réseau VMNet8.

LAN (10.0.0.x)



Host-only

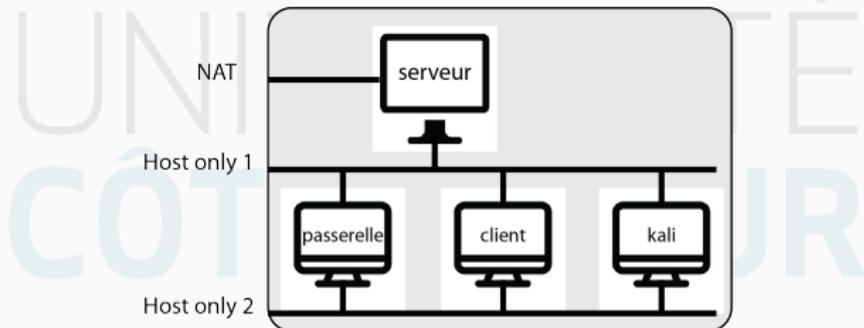
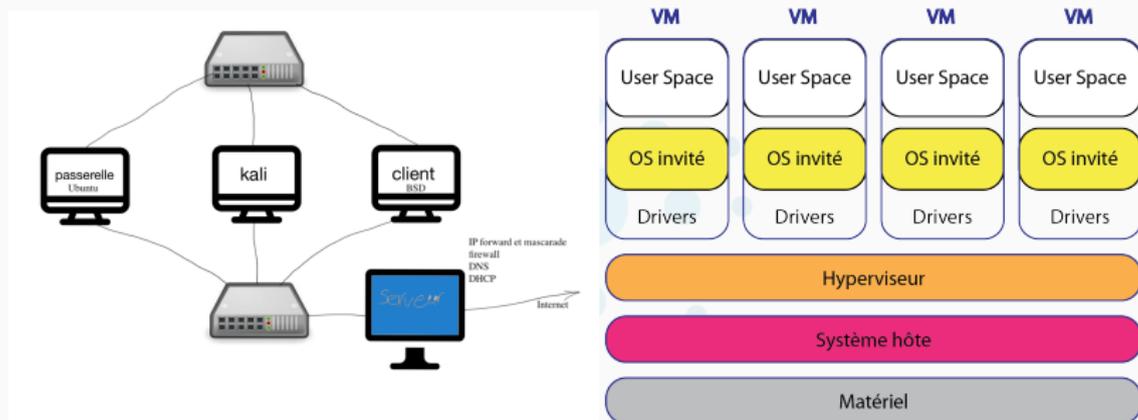
La machine virtuelle a accès uniquement à la machine hôte sur un réseau privé virtuel (VMNetX).
Vu du LAN, il n'y a aucune nouvelle machine.
La machine hôte fait office de serveur DHCP pour le réseau VMNet1.



Hyperviseur de type 2

UNIVERSITÉ
CÔTE D'AZUR

Virtualisation "simple" de l'environnement



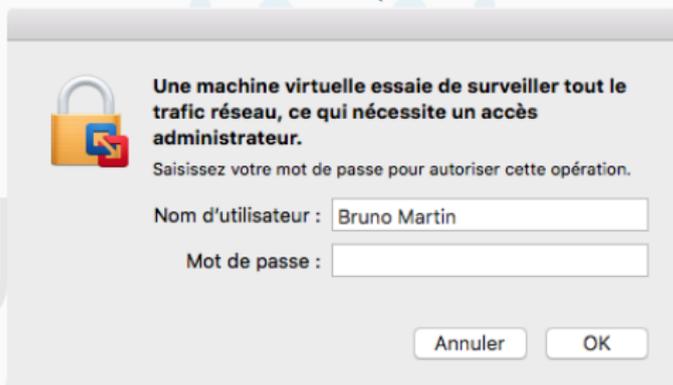
Hyperviseur de type 2

- + Réalisable facilement
- + Coût quasi-nul (VMWare Player gratuit)
 - Très difficile à déployer sur un parc (installation par machine)
 - Utilisation du réseau **incertain** (admin sur la machine)

UNIVERSITÉ
CÔTE D'AZUR

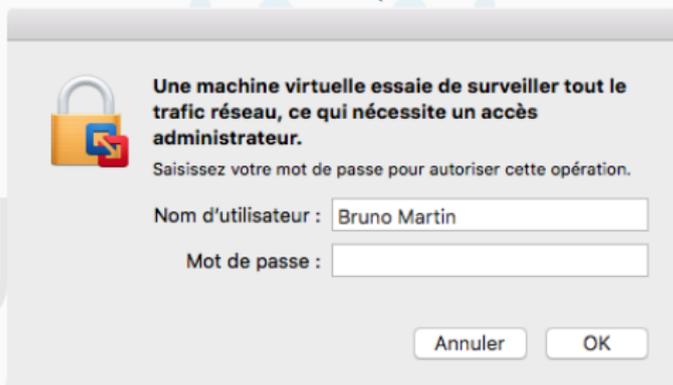
Hyperviseur de type 2

- + Réalisable facilement
- + Coût quasi-nul (VMWare Player gratuit)
 - Très difficile à déployer sur un parc (installation par machine)
 - Utilisation du réseau **incertain** (admin sur la machine)



Hyperviseur de type 2

- + Réalisable facilement
- + Coût quasi-nul (VMWare Player gratuit)
 - Très difficile à déployer sur un parc (installation par machine)
 - Utilisation du réseau **incertain** (admin sur la machine)



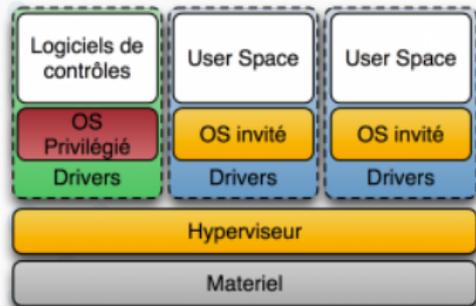
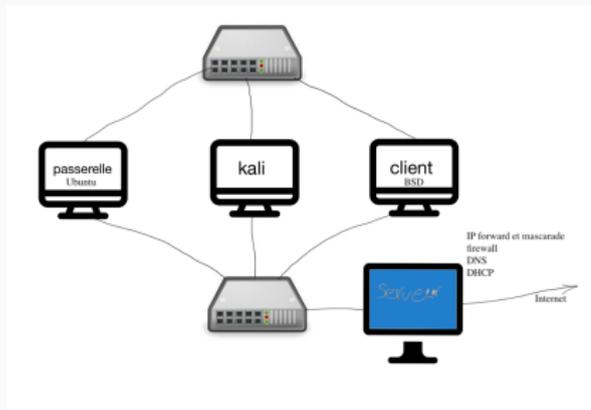
Remède : ajouter une couche de virtualisation !



Hyperviseur de type 1 virtualisé

UNIVERSITÉ
CÔTE D'AZUR

Virtualisons les VM !



Navigateur

- Hôte
 - Gérer
 - Surveiller
- Machines virtuelles 4
- Stockage 1
- Mise en réseau 3

localhost.localdomain - Mise en réseau

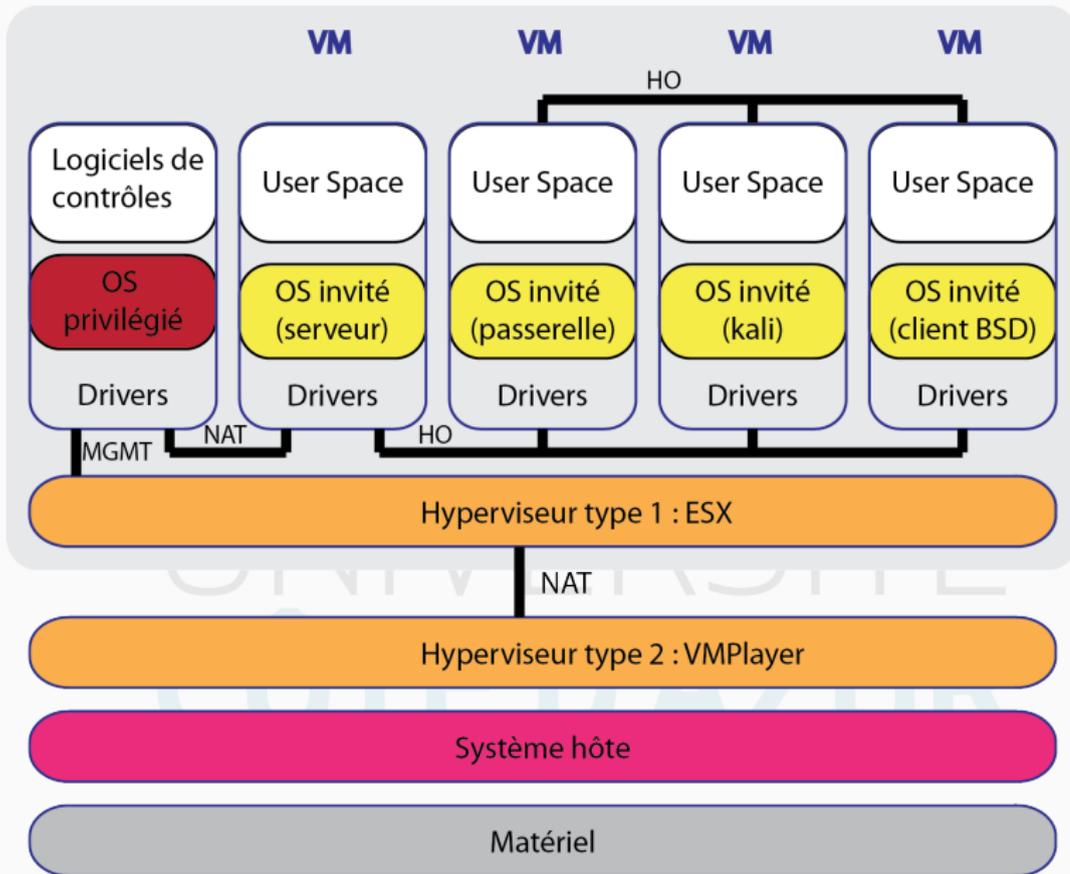
Groupes de ports Commutateurs virtuels NIC physiques NIC VMkernel

Recherche

Nom	P...	ID...	Type	vSwitch	VM
LANTP	3	1	Groupe de ports...	vSwitch0	3
VM Network	1	0	Groupe de ports...	vSwitch0	1
Managemen...	1	0	Groupe de ports...	vSwitch0	S/O
SLAN	4	0	Groupe de ports...	SLAN	4

4 éléments

Ajout d'une couche de virtualisation



Ajout d'une couche de virtualisation : résultat

The screenshot shows a window titled "MACHINES VIRTUELLES" with a sidebar listing "Windows 7" and "VMware ESXi 6" (IP: 172.16.250.147). The main area displays a terminal window with the following text:

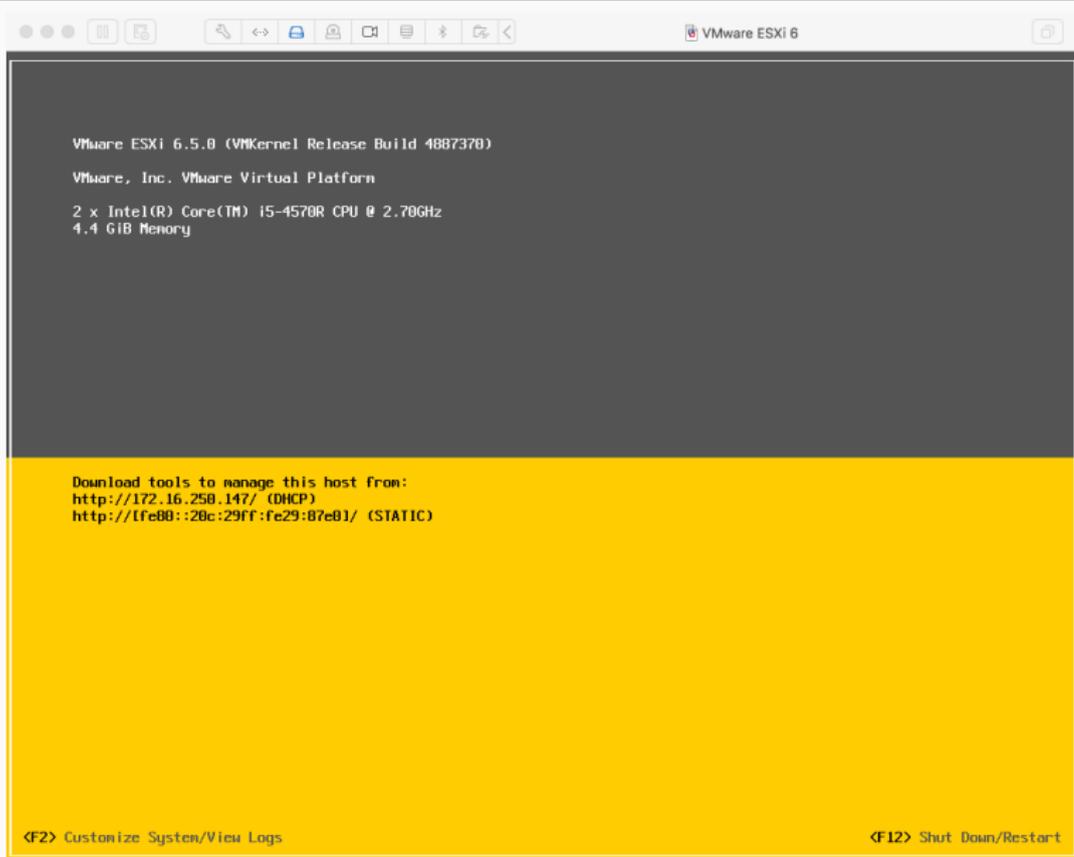
```
VMware ESXi 6.5.0 (Build-1) Release Build 4807391
VMware, Inc. VMware Virtual Platform
2 x Intel(R) Xeon(R) CPU @ 2.93GHz
1 x 64 Memory

Intel(R) Xeon(R) CPU @ 2.93GHz
VMware, Inc. VMware Virtual Platform
2 x Intel(R) Xeon(R) CPU @ 2.93GHz
1 x 64 Memory
```

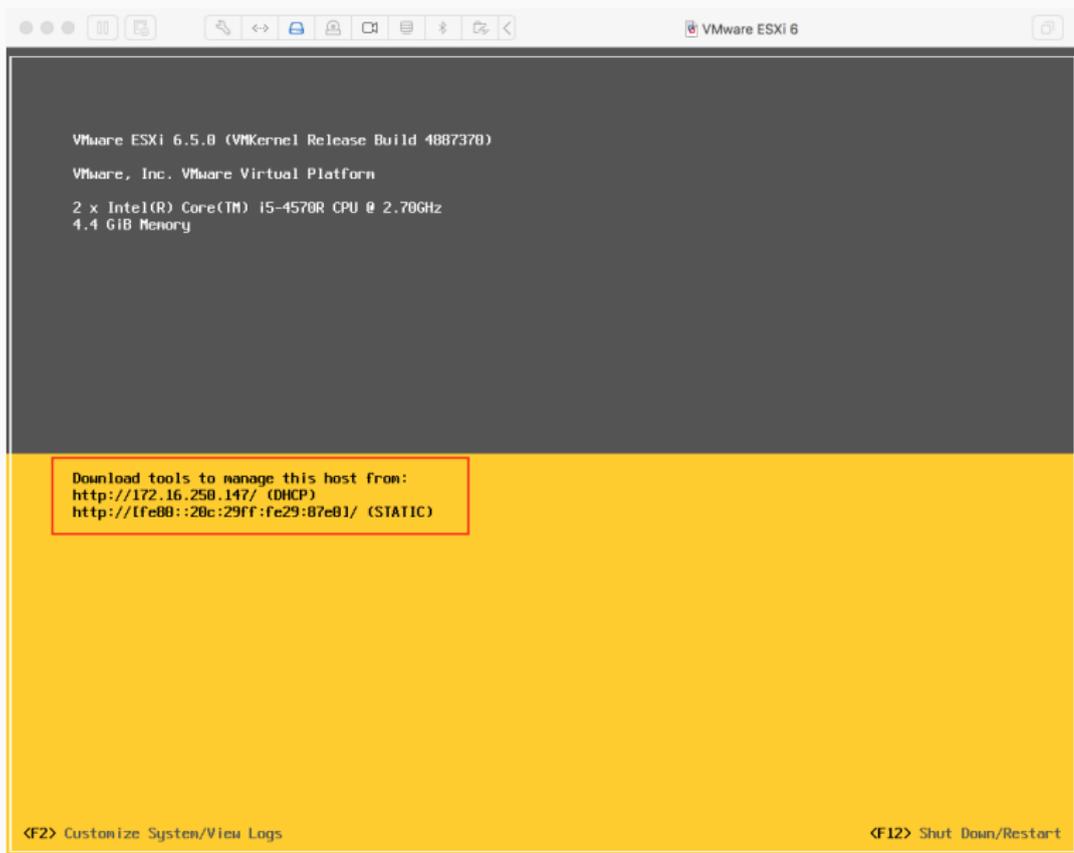
Below the terminal, the VMware ESXi 6.5.0 details are shown:

- VMware ESXi 6** (VMware ESXi 6.5.0)
- root / mdp ca...
- 2 cœurs de processeur
- 4540 Mo de mémoire
- Disques durs 30,6 Go
- Snapshots 0 octets
- Récupérable

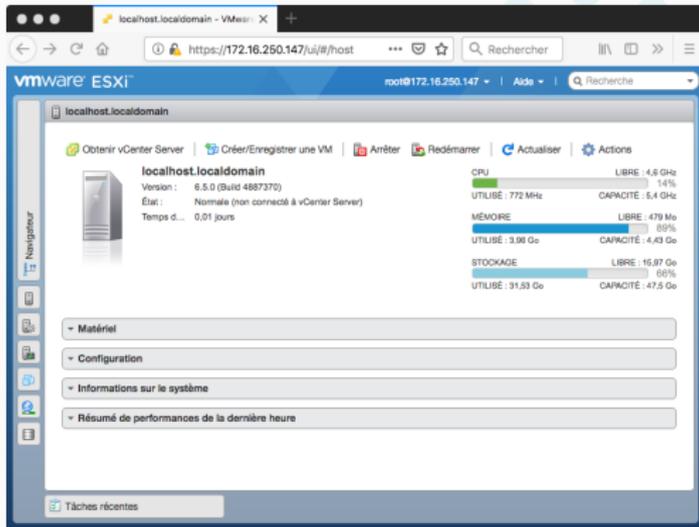
Ajout d'une couche de virtualisation : ESXi



Ajout d'une couche de virtualisation : ESXi

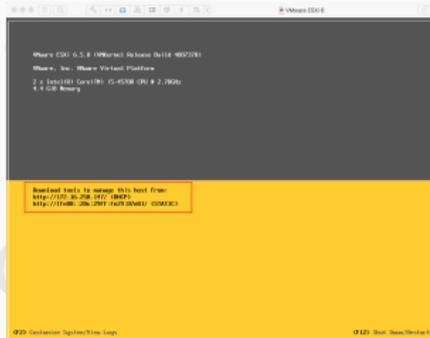


Connexion à l'ESXi



The screenshot shows the VMware ESXi web interface in a browser window. The address bar displays `https://172.16.250.147/ui/#/host`. The interface title is `localhost.localdomain`. The main content area displays system information for `localhost.localdomain`, including version `6.5.0 (Build 4887370)` and status `Normal (non connecté à vCenter Server)`. A navigation sidebar on the left includes options like `Matériel`, `Configuration`, `Informations sur le système`, and `Résumé de performances de la dernière heure`. On the right, system statistics are shown with progress bars:

Resource	Unit	Used	Capacity	Percentage
CPU	LIBRE	4,6 GHz	14%	
UTILISÉ		772 MHz		
MÉMOIRE	LIBRE	479 Mo	89%	
UTILISÉ		3,98 Go		
STOCKAGE	LIBRE	16,97 Go	60%	
UTILISÉ		91,93 Go		



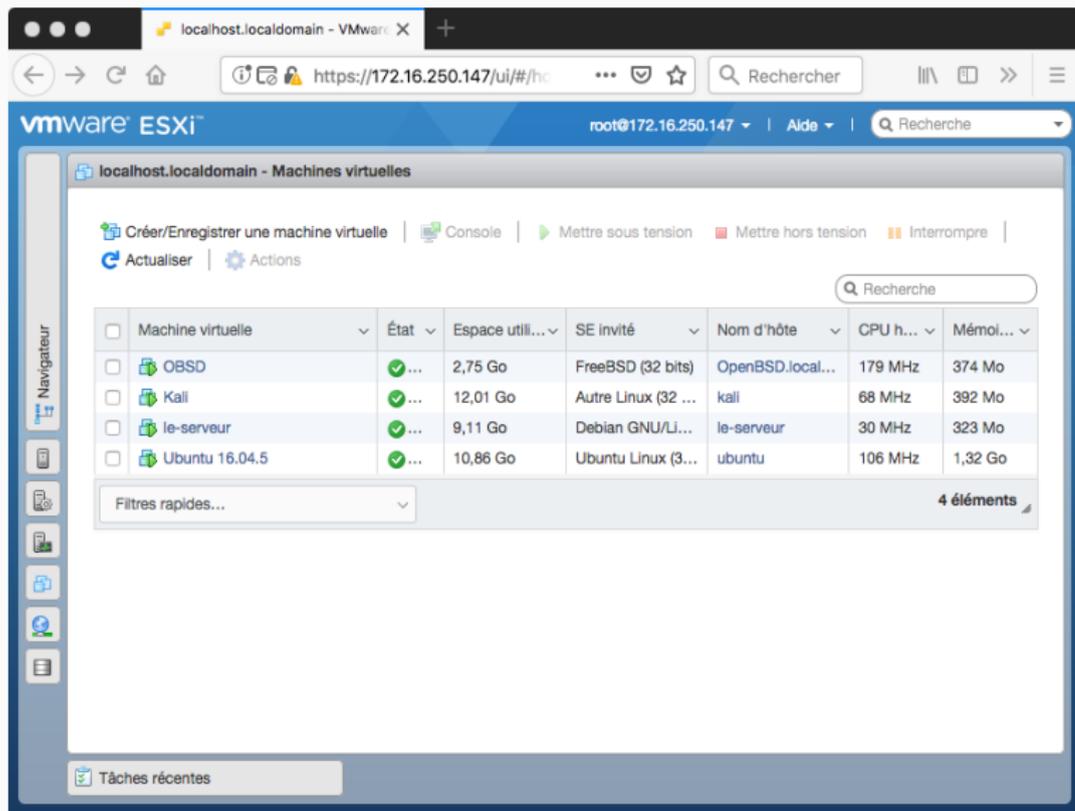
The screenshot shows a terminal window displaying system information for VMware ESXi 6.5.0. The text in the terminal is as follows:

```
VMware ESXi: 6.5.0 (VMware) Release Build 4887370
VMware, Inc. VMware Virtual Platform
3.0 (60018) Core119: 10-CPU, CPU @ 2.70GHz
4 x USB Mouse
```

Below the system information, there is a yellow box containing the following text:

```
Download links to upgrade this host from:
http://172.16.250.147/ESXi/
http://172.16.250.147/ESXi/ESX/
```

Connexion à l'ESXi : accès aux VM



The screenshot shows the VMware ESXi web interface in a browser window. The browser address bar displays `https://172.16.250.147/ui/#/hc`. The ESXi interface header shows `localhost.localdomain - VMware ESXi` and `root@172.16.250.147`. The main content area is titled `localhost.localdomain - Machines virtuelles` and contains a table of virtual machines.

Navigation and action buttons at the top include: `Créer/Enregistrer une machine virtuelle`, `Console`, `Mettre sous tension`, `Mettre hors tension`, `Interrompre`, `Actualiser`, and `Actions`.

The table lists the following virtual machines:

<input type="checkbox"/>	Machine virtuelle	État	Espace utilis...	SE Invité	Nom d'hôte	CPU h...	Mémoi...
<input type="checkbox"/>	 OSBD	✓ ...	2,75 Go	FreeBSD (32 bits)	OpenBSD.local...	179 MHz	374 Mo
<input type="checkbox"/>	 Kali	✓ ...	12,01 Go	Autre Linux (32 ...	kali	68 MHz	392 Mo
<input type="checkbox"/>	 le-serveur	✓ ...	9,11 Go	Debian GNU/LI...	le-serveur	30 MHz	323 Mo
<input type="checkbox"/>	 Ubuntu 16.04.5	✓ ...	10,86 Go	Ubuntu Linux (3...	ubuntu	106 MHz	1,32 Go

Below the table, there is a search bar labeled `Recherche` and a filter dropdown labeled `Filtres rapides...`. The bottom right of the table area indicates `4 éléments`.

A sidebar on the left contains a `Navigateur` menu and several icons. At the bottom left, there is a `Tâches récentes` button.

Connexion à l'ESXi : accès aux VM

The screenshot displays the VMware ESXi web interface in a browser window. The browser's address bar shows the URL `https://172.16.250.147/ui/#/hc`. The ESXi interface header includes the text "vmware ESXi™" and the user "root@172.16.250.147".

The main content area shows a virtual machine named "Ubuntu 16.04.5" with a desktop environment titled "Bureau Ubuntu". On the left side, there is a "Navigateur" (Navigator) pane with a list of virtual machines:

- Machine virtuelle
- OBSD
- Kali
- le-serveur
- Ubuntu 16.04.5

Below the list is a "Filtres rapides..." (Quick filters...) section. At the bottom of the navigator pane, there is a "Tâches récentes" (Recent tasks) section.

The desktop environment shows several application icons: a gear (Settings), a folder (Files), the Firefox browser, a briefcase (Applications), a gear with a wrench (Tools), and a terminal window.

Hyperviseur de type 1 virtualisé

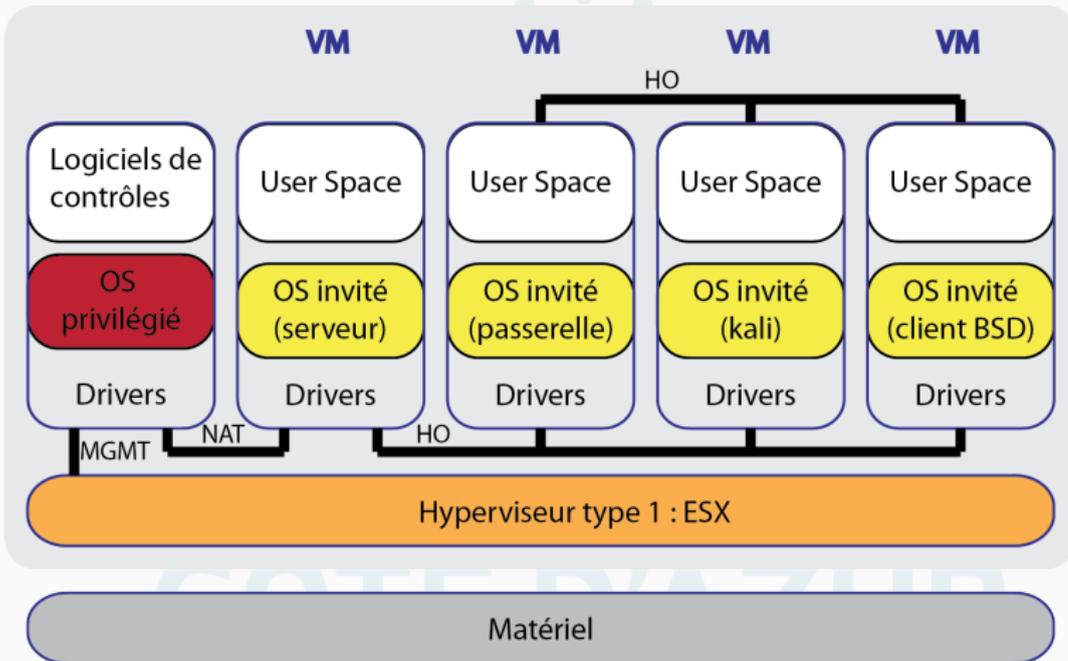
- + Coût quasi-nul (VMWare Player gratuit, licence ESXi gratuite)
- + Utilisation du réseau **sûre** (pas admin sur l'ESXi, \neq rôles)
- + Utilisable sur plusieurs OS hôtes (Win, MacOS, linux)
 - Réalisation assez technique
 - Laborieux à déployer sur un parc (recopie de gros volumes)
 - Limitation aux images 32 bits des distributions
 - Mise à jour laborieuse
 - Gestion de plusieurs groupes successifs quasi-impossible



Hyperviseur de type 1 (serveur)

UNIVERSITÉ
CÔTE D'AZUR

Avec un serveur de virtualisation



Hyperviseur de type 1 non virtualisé

- + Utilisation du réseau **sûre** (pas admin sur l'ESXi)
- + Utilisable sur plusieurs OS hôtes (Win, MacOS, linux)
- + Pas de problème de déploiement
- + Pas de limitation aux images 32 bits des distributions
- + Possibilité d'interconnecter tout le monde (MAN)
- + Mises à jour facilitées
 - Coût important (achat serveur, licence ESXi payante)
 - Support technique (IE ou IR)
 - Réalisation assez technique

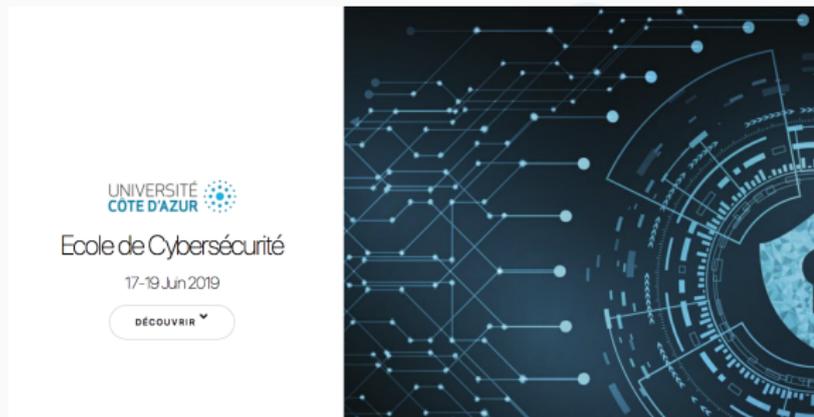
Conclusion



UNIVERSITÉ
CÔTE D'AZUR

Conclusion

	salle	type 2	type 1V	type 1
coût	€€€	0	0	€€
droits	root	root hôte	user	user
déploiement	*	**	*	***
portabilité	-	*	**	-
flexibilité	-	***	**	****
technicité	***	*	**	**
DNS local	oui	non	oui	oui
support	IE/IR	-	-	IE/IR
màj	*	***	**	***
32/64	oui	oui	non	oui



UNIVERSITÉ
CÔTE D'AZUR

Ecole de Cybersécurité

17-19 Jun 2019

DÉCOUVRIR

The banner features a dark blue background with a network of glowing blue nodes and lines on the left, and a circular digital interface with various data points and lines on the right.



<http://univ-cotedazur.fr/events/ecole-cybersecurite-2019>

CÔTE D'AZUR